



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/067,610	02/04/2002	Rafie Shamsaasef	D2684	5884

43471 7590 10/16/2006

GENERAL INSTRUMENT CORPORATION DBA THE CONNECTED  
HOME SOLUTIONS BUSINESS OF MOTOROLA, INC.  
101 TOURNAMENT DRIVE  
HORSHAM, PA 19044

EXAMINER
----------

OKORONKWO, CHINWENDU C

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 10/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 10/067,610	<b>Applicant(s)</b> SHAMSAASEF ET AL.	
	<b>Examiner</b> Chinwendu C. Okoronkwo	<b>Art Unit</b> 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☐ Responsive to communication(s) filed on 07 August 2006.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1 and 3-20 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1 and 3-20 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |                                                                                                            |                                                                                         |
|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                                           | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____                                                |

## DETAILED ACTION

### *Response to Arguments*

1. In response to communications filed on 8/7/2006, applicant does amend claims 1, 3, 8, 10-12 and 14-16. The following claims, claims 1 and 3-20 are presented for examination.

1.1 Applicant's arguments, pages 8-9, with respect to the rejection of claims 1 and 3-20 have been fully considered but they are not persuasive.

1.2 In response to Applicant argument that the Brezak et al. and Kato references do not teach or suggest a server which both issues service tickets and receives requests for access information to access content, the Examiner respectfully disagrees citing paragraph 0035, 0045 and 0048 of Brezak et al. which clearly recites, "having possession of a client's ticket granting ticket (TGT) and associated authenticator **allows the holder to request tickets** on behalf of the client **from the trusted third-party, e.g., a key distribution center (KDC)** (0035)." Brezak further recites, "**server A 210** sends a TGS\_REQ message 230 to authentication service 206. **TGS\_REQ message 230 includes** the TGT for server A 210 and **the service ticket** received from client 202, **and [access information for] the desired or targeted server/service seeking access** (0045)." Brezak goes even further to recite, "authentication service 206 accessed the similar/**necessary client information** in database 208 after being satisfied that the

Art Unit: 2136

authenticated client is essentially involved in the request **based on the service ticket that authenticated server A 210 received from client 202** and included in TGS\_REQ message 230 (0048).” Applicant has not overcome the rejection.

***Claim Rejections - 35 USC § 102***

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1, 4 and 5 are rejected under 35 U.S.C. 102(e) as being disclosed by Brezak et al. (U.S. Patent Publication No. 20030018913).

Regarding claim 1, Brezak et al., discloses a communication authorization method, comprising the steps of:

- A third party server receiving a request for access information to access content (0042);
- generating the access information to access the desired content from a first application server, wherein the first service ticket is obtained from a key distribution center (0045);
- generating authentication of the access information using a first service ticket to the first application server (0046-0048); and
- sending the access information and authentication to a client, whereby the client presents the access information and authentication to the first application server to be authorized to receive the desired content from the first application server (0048).

Regarding claim 4, Brezak et al., discloses the method as claimed in claim 1, further comprising the step of: generating at least a portion of the authentication using the first service ticket (0048).

Regarding claim 5, Brezak et al., discloses the method as claimed in claim 4, further comprising the steps of:

- requesting a ticket granting ticket (TGT ticket) (0004);
- receiving a TGT ticket (0005);
- requesting the third party server service ticket for the first application server (0008); and
- receiving the third party server service ticket for the first application server (0008).

***Claim Rejections - 35 USC § 103***

3. Claims 3 and 6-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brezak et al. as applied to claims 1, 4 and 5 above, and further in view of Kato (US Patent Number 6,381,331 B1).

Regarding claim 3, Brezak et al. is silent in disclosing the step of generating the access information includes generating session rights and encrypting at least a portion of the session rights using a third party server service key for the first application server.

Kato discloses an "information sending system and method, which can send encrypted information which can be decrypted in units of portions of the

information,” comprising information (access information) segmentation means for segmenting information into a plurality of blocks and encrypting the plurality of segmented blocks (portion of the session rights) using a first key (third party server service key) (col. 1 lines 47-63 of Kato).

It would have been obvious to a person of ordinary skill in the art, at the time of the invention, to have been motivated to apply the information segmentation and first key encryption means of Kato with the system and method for constrained delegation of authentication credentials of Brezak et al. Motivation for this combination is recited by Kato whereby it is disclosed that the information sending system, of Kato, encrypts outgoing information with different keys, and the first and second keys for decrypting these blocks are encrypted by different keys and are added to the outgoing information, allowing for different persona to either have the ability to decrypt blocks of information encoded with either one or both keys – it allows for added security (col. 2 lines 19-29). Therefore, Brezak et al. presents a method for constrained delegation of authentication credentials without explicitly reciting the features of security inherent in an authentication service (server) – although implied due to the basic functionality of an authentication server. Kato explicitly recites these security features which comprise the claimed security features of the applicant as noted above.

Regarding claim 6, Brezak et al., the method as claimed in claim 1, further comprising the steps of:

- verifying the authentication of the access information using the first service ticket, and client authorization (0046-0048 of Brezak et al.); and
- issuing a key reply if the authentication of the access information and client authorization are verified (0048 of Brezak et al.).

Brezak et al. are silent in disclosing the extracting the access information and authentication.

Kato does disclose the extracting the access information and authentication (col. 11 lines 22-27 Kato).

It would have been obvious to a person of ordinary skill in the art to have been motivated to apply the steps of extracting a session key of Kato with the system and method for constrained delegation of authentication credentials of Brezak et al. Brezak et al. recites motivation for this combination whereby it is disclosed "a method that includes identifying a target service (server) to which access is sought on behalf of a client, and causing a server to request a new service credential (key), for use by the server, from a trusted third-party" (0008 of Brezak et al.). Therefore, it would have been obvious to combine the steps of extracting a session key of Kato with the system and



method for constrained delegation of authentication credentials of Brezak et al., as the system and methods of Brezak et al. incorporates the transmission of a key request in the request for a “new service credential” – although not explicitly stating this key would be “extracted” and sent to the requester.

Brezak et al. are silent in disclosing the application server receiving a key request including the access information and authentication.

Kato does disclose the delivery of the public key to users, delivery of secret key information and notification of download request (key request) (col. 9 lines 64-67, col. 10 lines 1-4, col. 10 lines 64-67 and col. 11 lines 1-2 of Kato).

It would have been obvious to a person of ordinary skill in the art to have been motivated to apply the download request (key request) delivery system of Kato with the system and method for constrained delegation of authentication credentials of Brezak et al. Brezak et al. recites motivation for this combination whereby it is disclosed “a method that includes identifying a target service (server) to which access is sought on behalf of a client, and causing a server to request a new service credential (key), for use by the server, from a trusted third-party (0008 of Brezak et al.). Kato, as cited above, explicitly recites this limitation. Therefore, Brezak et al., discloses the method for constrained delegation of authentication credentials – implying use

of a means for authentication such as the claimed “key” of the applicant.

Kato explicitly recites usage of the download request analogous in functionality to the key request, which it would have been obvious to combine with the above method for constrained delegation of authentication credentials of Brezak et al.

Regarding claim 7, Brezak et al., the method as claimed in claim 6, further comprising the steps of:

- sending the key request to the first application server (0042 of Brezak et al.); and
- receiving the key reply (KEY\_REP) if the authentication of the access information and client authorization are verified by the first application server (0048 of Brezak et al.).

[The Examiner’s Reasoning: Because the key is included in the transmission of authentication information, the term “KEY\_REP” the Applicant claim is analogous to “TGS\_REP” of Brezak et al.]

Brezak et al. are silent in disclosing a client generating a key request including the access information and the authentication.

- Kato does disclose a client generating a key request including the access information and the authentication (col. 9 lines 64-67, col. 10 lines 1-4, col. 10 lines 64-67 and col. 10 lines 1-2 of Kato);

[*The Examiner's Reasoning*: The server receiving a key request implies that the request must first be generated by the requests of the client.]

It would have been obvious to a person of ordinary skill in the art to have been motivated to apply the download request (key request) delivery system of Kato with the system and method for constrained delegation of authentication credentials of Brezak et al. Brezak et al. recites motivation for this combination whereby it is disclosed "a method that includes identifying a target service (server) to which access is sought on behalf of a client, and causing a server to request a new service credential (key), for use by the server, from a trusted third-party (0008 of Brezak et al.). Kato, as cited above, explicitly recites this limitation. Therefore, Brezak et al., discloses the method for constrained delegation of authentication credentials – implying use of a means for authentication such as the claimed "key" of the applicant. Kato explicitly recites usage of the download request analogous in functionality to the key request, which it would have been obvious to combine with the above method for constrained delegation of authentication credentials of Brezak et al.

Regarding claim 8, Brezak et al., discloses a method for verifying authorization for a client to gain access to content and/or services, comprising the steps of:

- extracting third party server access information and third party server authentication from the key request from a client (col. 11 lines 22-27 Kato);
- verifying an authentication of the third party access information and a client authorization (0046-0048 of Brezak et al.); and
- issuing a key reply if the authentication of the third party access information and the client authorization are verified (0048 of Brezak et al.).

Brezak et al. are silent in disclosing receiving a key request.

Kato does disclose the receiving a key request (col. 9 lines 64-67, col. 10 lines 1-4, col. 10 lines 64-67 and col. 11 lines 1-2 of Kato).

It would have been obvious to a person of ordinary skill in the art to have been motivated to apply the steps of extracting a session key of Kato with the system and method for constrained delegation of authentication credentials of Brezak et al. Brezak et al. recites motivation for this combination whereby it is disclosed "a method that includes identifying a target service (server) to which access is sought on behalf of a client, and causing a server to request

a new service credential (key), for use by the server, from a trusted third-party" (0008 of Brezak et al.). Therefore, it would have been obvious to combine the steps of extracting a session key of Kato with the system and method for constrained delegation of authentication credentials of Brezak et al., as the system and methods of Brezak et al. incorporates the transmission of a key request in the request for a "new service credential" – although not explicitly stating this key would be "extracted" and sent to the requester.

Regarding claim 9, Brezak et al., discloses the method as claimed in claim 8, further comprising the step of authenticating the third party server access information using the third party server authentication (0043 and 0048 of Brezak et al.).

Regarding claim 10, Brezak et al., discloses the method as claimed in claim 9, wherein the step of authenticating includes extracting a first service ticket and authenticating the third party server access information using the first service ticket (0055 of Brezak et al.).

[The Examiner's Reasoning: The disclosed forwarding of the service ticket implies extracting service ticket as a ticket must be isolated/extracted before being forwarded.]

Regarding claim 11, Brezak et al., discloses the method as claimed in claim 8, wherein the step of extracting the third party server authentication, further comprising:

Brezak et al. are silent in disclosing the step of authenticating the access information includes verifying a third party server signature using the session key.

Kato does disclose the step of authenticating the access information including verifying a third party server signature using the session key (col. 6 lines 42-49).

It would have been obvious to a person of ordinary skill in the art to have been motivated to apply the step of generating the authentication including generating a signature utilizing a session key of the third party server service ticket of Kato with the system and method for constrained delegation of authentication credentials of Brezak et al. Kato recites a motivation for the combination, whereby disclosing an information sending system and mail wherein data to be sent from sender A is broken up into a plurality of blocks and a transmission packet is formed from those blocks which are encrypted to be decryptable by the administrator and the receiver, and blocks which are encrypted to be decryptable by the receiver only. Thus, the encrypted key

(session key) is encrypted with the public key of the administrator – producing a signature of the administrator of the third party server. Therefore, it would have been obvious to combine the steps of generating a signature utilizing a session key of the third party server service ticket of Kato with the system and method for constrained delegation of authentication credentials of Brezak et al., as the system and methods of Brezak et al. incorporate the key request and Kato makes use of this key in the generation of signatures, encrypting the said key with the administrator's producing a signature.

Brezak et al. are silent in disclosing the steps of extracting a session key from the key request.

Kato does disclose the steps of extracting a session key from the key request (col. 9 lines 64-67, col. 10 lines 1-4, col. 10 lines 64-67 and col. 11 lines 6-52 of Kato).

It would have been obvious to a person of ordinary skill in the art to have been motivated to apply the steps of extracting a session key of Kato with the system and method for constrained delegation of authentication credentials of Brezak et al. Brezak et al. recites motivation for this combination whereby it is disclosed "a method that includes identifying a target service (server) to which access is sought on behalf of a client, and causing a server to request

a new service credential (key), for use by the server, from a trusted third-party" (0008 of Brezak et al.). Therefore, it would have been obvious to combine the steps of extracting a session key of Kato with the system and method for constrained delegation of authentication credentials of Brezak et al., as the system and methods of Brezak et al. incorporates the transmission of a key request in the request for a "new service credential" – although not explicitly stating this key would be "extracted" and sent to the requester.

Regarding claim 12, Brezak et al. are silent in disclosing the method as claimed in claim 11, wherein the step of extracting the session key includes decrypting at least a portion of the key request using an application server service key and extracting the session key.

Kato does disclose disclosing the method as claimed in claim 11, wherein the step of extracting the session key including decrypting at least a portion of the key request using an application server service key and extracting the session key (col. 11 lines 6-52 and col. 12 lines 1-5 of Kato).

It would have been obvious to a person of ordinary skill in the art to have been motivated to apply the steps of extracting a session key of Kato with the system and method for constrained delegation of authentication credentials of Brezak et al. Brezak et al. recites motivation for this combination whereby it



is disclosed “a method that includes identifying a target service (server) to which access is sought on behalf of a client, and causing a server to request a new service credential (key), for use by the server, from a trusted third-party” (0008 of Brezak et al.). Therefore, it would have been obvious to combine the steps of extracting a session key of Kato with the system and method for constrained delegation of authentication credentials of Brezak et al., as the system and methods of Brezak et al. incorporates the transmission of a key request in the request for a “new service credential” – although not explicitly stating this key would be “extracted” and sent to the requester.

Regarding claim 13, Brezak et al., discloses the method as claimed in claim 8, further comprising the steps of:

- the third party server receiving a request for the access information to access content (0042 of Brezak et al.);
- generating the third party server access information to access the desired content from a first application server (0045 of Brezak et al.); and
- generating the third party server authentication of the access information (0046-0048 of Brezak et al.).

Regarding claim 14, Brezak et al., discloses the method as claimed in claim 13, wherein the step of generating the third party server authentication includes

incorporating a third party server service ticket for the first application server (0043-0045 of Brezak et al.).

Regarding claim 15, Brezak et al., is silent in disclosing the method as claimed in claim 14, wherein the step of generating the authentication includes generating a signature utilizing a session key of the third party server service ticket.

Kato does disclose the method as claimed in claim 14, wherein the step of generating the authentication including generating a signature utilizing a session key of the third party server service ticket (col. 6 lines 42-49).

It would have been obvious to a person of ordinary skill in the art to have been motivated to apply the step of generating the authentication including generating a signature utilizing a session key of the third party server service ticket of Kato with the system and method for constrained delegation of authentication credentials of Brezak et al. Kato recites a motivation for the combination, whereby disclosing an information sending system and mail wherein data to be sent from sender A is broken up into a plurality of blocks and a transmission packet is formed from those blocks which are encrypted to be decryptable by the administrator and the receiver, and blocks which are encrypted to be decryptable by the receiver only. Thus, the encrypted key (session key) is encrypted with the public key of the administrator – producing

a signature of the administrator of the third party server. Therefore, it would have been obvious to combine the steps of generating a signature utilizing a session key of the third party server service ticket of Kato with the system and method for constrained delegation of authentication credentials of Brezak et al., as the system and methods of Brezak et al. incorporate the key request and Kato makes use of this key in the generation of signatures, encrypting the said key with the administrator's producing a signature.

Regarding claim 16, Brezak et al., discloses the method as claimed in claim 14, wherein the steps of verifying the authentication of the access information includes verifying the third party server service ticket (0043-0048 of Brezak et al.).

Brezak et al. are silent in disclosing the extraction of the third party server service ticket.

Kato does disclose disclosing the extraction of the third party server service ticket (col. 111 lines 22-27 of Kato).

It would have been obvious to a person of ordinary skill in the art to have been motivated to apply the steps of extracting a session key of Kato with the system and method for constrained delegation of authentication credentials of

Brezak et al. Brezak et al. recites motivation for this combination whereby it is disclosed “a method that includes identifying a target service (server) to which access is sought on behalf of a client, and causing a server to request a new service credential (key), for use by the server, from a trusted third-party” (0008 of Brezak et al.). Therefore, it would have been obvious to combine the steps of extracting a session key of Kato with the system and method for constrained delegation of authentication credentials of Brezak et al., as the system and methods of Brezak et al. incorporates the transmission of a key request in the request for a “new service credential” – although not explicitly stating this key would be “extracted” and sent to the requester.

Regarding claim 17, Brezak et al., discloses a method for providing secure communication when distributing services, comprising: the steps of:

- a third party server receiving a selection for services (0042 of Brezak et al.);
- issuing access information for the services (0045 of Brezak et al.);
- issuing authentication of the access information (0046-0048 of Brezak et al.);
- verifying an authentication of the access information and a client authorization utilizing, at least in part, a first service ticket (0048 of Brezak et al.); and

- issuing a key reply to a client if the authentication of the access information and the client authorization are verified (0048 of Brezak et al.).

Brezak et al. are silent in disclosing an application server receiving a key request from a client.

Kato does disclose the delivery of the public key to users, delivery of secret key information and notification of download request (key request) (col. 9 lines 64-67, col. 10 lines 1-4, col. 10 lines 64-67 and col. 11 lines 1-2 of Kato).

It would have been obvious to a person of ordinary skill in the art to have been motivated to apply the steps of extracting a session key of Kato with the system and method for constrained delegation of authentication credentials of Brezak et al. Brezak et al. recites motivation for this combination whereby it is disclosed "a method that includes identifying a target service (server) to which access is sought on behalf of a client, and causing a server to request a new service credential (key), for use by the server, from a trusted third-party" (0008 of Brezak et al.). Therefore, it would have been obvious to combine the steps of extracting a session key of Kato with the system and method for constrained delegation of authentication credentials of Brezak et al., as the system and methods of Brezak et al. incorporates the transmission

of a key request in the request for a “new service credential” – although not explicitly stating this key would be “extracted” and sent to the requester.

Regarding claim 18, Brezak et al., discloses the method as claimed in claim 17, further comprising the steps of:

- a KDC receiving a first service ticket request from a third party server for the application server (0137 and 0141 of Brezak et al.);
- a KDC issuing the first service ticket to the third party server for the application server (0085 of Brezak et al.); and
- the steps of the third party issuing access information and authentication including generating the access information and authentication using the first service ticket (0015 and 0016 of Brezak et al.).

Regarding claim 19, Brezak et al., discloses the method as claimed in claim 17, further comprising the steps of:

- receiving a second service ticket request for the first server (claims 36 and 40 of Brezak et al.);
- issuing a second service ticket for the application server (claims 36 and 40 of Brezak et al.); and
- the step of the application server receiving a key request wherein the key request includes the second service ticket (claims 36 and 40 of Brezak et al.).

Regarding claim 20, Brezak et al., discloses the method as claimed in claim 17, wherein: the step of verifying the authentication of the access information includes:

- extracting the first service ticket (0055 of Brezak et al.);
- generating a signature using the session key (0046-0048 of Brezak et al.);

Brezak et al. are silent in disclosing the following limitations:

- decrypting the first service ticket;
- extracting a session key from the first service ticket;
- verifying the signature over the access information with the session key.

Kato does disclose the following limitations:

- decrypting the first service ticket (col. 2 lines 19-23 of Kato);
- extracting a session key from the first service ticket (col. 11 lines 6-52 of Kato);
- verifying the signature over the access information with the session key (col. 6 lines 42-49 of Kato).

It would have been obvious to a person of ordinary skill in the art to have been motivated to apply the steps of extracting a session key of Kato with the system and method for constrained delegation of authentication credentials of Brezak et

al. Brezak et al. recites motivation for this combination whereby it is disclosed “a method that includes identifying a target service (server) to which access is sought on behalf of a client, and causing a server to request a new service credential (key), for use by the server, from a trusted third-party” (0008 of Brezak et al.). Therefore, it would have been obvious to combine the steps of extracting a session key of Kato with the system and method for constrained delegation of authentication credentials of Brezak et al., as the system and methods of Brezak et al. incorporates the transmission of a key request in the request for a “new service credential” – although not explicitly stating this key would be “extracted” and sent to the requester.

The prior art made of record, although not relied upon, and considered pertinent to applicant’s disclosure include:

U.S. Patent(s):

6,775,772	<u>Binding et al.</u>
5,832,228	<u>Holden et al.</u>
6,067,620	<u>Holden et al.</u>
5,872,849	<u>Sudia, Frank Wells</u>
6,009,177	<u>Sudia, Frank Wells</u>
6,684,331	<u>Srivastava, Sunil K.</u>

U.S Patent Application Publication(s):



20030018915	<u>Stoll, Louis</u>
20030028762	<u>Trill et al.</u>
20040003287	<u>Zissimopoulos et al.</u>
20050114666	<u>Sudia, Frank W.</u>

### Conclusion

4. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chinwendu C. Okoronkwo whose telephone number is (571) 272 2662. The examiner can normally be reached on MWF 9:30 - 7:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272 4195. The fax phone

Art Unit: 2136

number for the organization where this application or proceeding is assigned is 571-273-8300.


Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



CCO

October 12, 2006

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

  
10/12/06